IN THE SPECIFICATION:

On Page 1 between original lines 2 and 3 insert "Field of the Invention".

Heading with markings:

Field of the Invention

Heading without markings:

Field of the Invention

On Page 1 between original lines 4 and 5 insert "Background".

Heading with markings:

Background

Heading without markings:

Background

IN THE SPECIFICATION:

On Page 7 line 12, after "IP address." please insert, --"Honeypot computer 12 includes one or more processors 31, Random Access Memory 32, operating system 33 and Read Only Memory 34 on a bus 35, and a disk storage device 36 coupled to bus 35. "--

Paragraph with markings:

Referring now to the drawings in detail wherein like reference numbers indicate like elements throughout, Figure 1 illustrates a computer system generally designated 10. System 10 comprises a multiplicity of known work stations 11a,b,c on an intranet 14. By way of example, intranet 14 is an Ethernet intranet, although intranet 14 could alternately be an Ethernet Internet, Ethernet private network, TokenRing Network, etc. System 10 also comprises a honeypot 12 connected to the intranet 14. Honeypot 12 receives messages from Internet 20 via the intranet 14. Typically, the messages are in the form of ATM packets where a sequence of packets forms each message. However, the present invention will accommodate other types of packets and messages as well. Honeypot 12 can be a server, workstation, embedded device such as a Single Board Computer (SBC), USB hard drive or other custom computer, small network appliance or other electronic device with an IP address. Honeypot computer 12 includes one or more processors 31, Random Access Memory 32, operating system 33 and Read Only Memory 34 on a bus 35, and a disk storage device 36 coupled to bus 35. Honeypot 14 preferably has an unused IP address, i.e. the device has no function that requires input or service from any other server or workstation, the IP address is not registered with a domain name service, and the IP address is not sent or broadcast to other servers or workstations. So, any packets, particularly non broadcast packets, sent to the honeypot 12 are unexpected and therefore, suspect. Intranet 14 is connected to the Internet 20 via firewall 22, such that honeypot 12 (and workstations 11a,b,c) is coupled to the Internet to receive IP packets from other devices (i.e. servers, workstations, routers, etc.) on or coupled to the Internet. By way of example, firewall 22 performs the following functions to limit what packets can pass from the Internet 20 to the intranet 14: accepts packets only from certain IP

protocols, sends packets only to certain ports, accepts packets only from certain IP addresses, denies traffic from entire subsets of IP addresses and accepts packets only from certain applications, in addition to many other similar functions. However, if desired, honeypot 12 can be directly connected to the Internet 20 without an intervening intranet and/or firewall.

On Page 8 line 11, after "distributed." please insert, --" Program 30 is stored in disk storage device 36 for execution by one or more processors 31 via RAM 32."--

Paragraph with markings:

In accordance with the present invention, honeypot 12 includes a honeypot packet filtering program 30 (Figure 2) which reviews all packets received by the honeypot 12, and filters out those packets which are not portions of exploits (i.e. computer viruses, worms, exploitation programs, etc.), or which are portions of old exploits with known signatures. A known security operations station ("SOC") 40 is coupled to the intranet 14 and to honeypot 12. The SOC includes human analysts which review exploit or intrusion alerts for authenticity. If an intrusion is deemed authentic, or not a false positive, the customer is called and informed that they are under attack. Honeypot 12 sends to SOC 40 only those packets which pass through the filtering program 30, and therefore warrant further analysis as portions of potential new exploits. It is not necessary for SOC 40 to analyze the packets which are not portions of exploits because they do not pose a security concern. Also, it is not necessary for SOC 40 to analyze the packets which are portions of known/old exploits because they have already been detected, and the respective anti virus, anti worm or anti exploitation program software has already been created and distributed. Program 30 is stored in disk storage device 36 for execution by one or more processors 31 via RAM 32.